REMARKS

The present Amendment amends claims 1, 2 and 4-6. Therefore, the present application has pending claims 1, 2 and 4-6.

In the Office Action, the Examiner rejected claims 1, 2 and 4-6 under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement and rejected Claims 1, 2 and 6 under 35 U.S.C. § 101 as be directed to non-statutory subject matter.

With respect to the rejection of claims 1, 2 and 4- 6 under § 112, first paragraph the Examiner took the position that the claims contain subject matter not in the specification in such a way as to reasonably convey to one skilled in the art that the inventors had possession of the claimed invention at the time the application was filed.

The subject matter as recited in the claims was in fact sufficiently described in the present application at the time it was originally filed. For example, the specification describes on page 11, lines 2-13 that:

> "In FIG. 5, the number "m" denotes a bit length necessary for storing the input x and "n" denotes a bit length necessary for storing P. The number m is necessarily larger than or equal to n (m.gtoreq.n) since 0<x<P*Q. First, U=2{circumflex over ( )}m mod P and U_SQR=2{circumflex over ( )}(2n)U mod P are calculated (5030). Incidentally, the above symbol "_" is used in this document to mean subscript. A detailed processing flow for calculating U_SQR=2{circumflex over ( )}(2n)U mod P is shown in FIG. 7. While FIG. 7 shows a procedure for calculating 2*U mod P, it can be used directly by substituting 2n into L (L=2n). The bit length of U_SQR equals that of the longer one of m-2n and n."

And on page 16, lines 1-2 that:

"Meanwhile, if we define "s" as the number of most significant bits 0 when Y is stored in m-bit memory"

The above noted passages of the present application describe the storing modulus P in a memory of at least n bits sufficient for storing the modulus P, storing the input value x in the memory which is also of at least m bits sufficient for storing the input value x and storing 2^(2m+n) mod P in the memory, and performing various Montgomery modular multiplications and the storing or data in an m-bit memory. In other words the specification clearly describes the storing of the modulus P and the input value x, the performing of Montgomery modular multiplications and an m-bit memory.

Thus, the subject matter as recited in the claims was in fact sufficiently described in the present application at the time it was originally filed in such a way as to reasonably convey to one skilled in the art that the inventors had possession of the claimed invention at the time the application was filed. Therefore, reconsideration and withdrawal of the 35 U.S.C. § 112, first paragraph rejection of claims 1, 2 and 4-6 is respectfully requested.

With respect to the rejection of claims 1, 2 and 6 under 35 U.S.C § 101, the Examiner alleges that the claims are directed to non-statutory subject matter. Applicants submit that amendments were made to the claims so as to more clearly describe that the present invention is directed to specific apparatus which implements the method and other functions/processes recited in the claims as permitted under 35 U.S.C § 101.

For example, the amendments now more clearly recite that the present invention is directed to an information processing method implemented by an information processing apparatus which forms a part of a tamper storage resistant storage device, and the information processing apparatus included in

the tamper resistant storage device. As per the present invention the tamper resistant storage device can be an IC card having high confidentiality.

According to the present invention the information processing apparatus included as part of the tamper resistant storage device performs the encryption of data to be input and stored on the tamper resistant storage. As per the present invention the information processing apparatus calculates x*(2^n) mod P for an input value x larger than a prime number P without directly obtaining x*(2^n) mod P of the input value x divided by P. By not directly obtaining x*(2^n) mod P of the input value x divided by P as per the present invention, the estimation of P becomes difficult. Accordingly, the tampering of the tamper resistant storage device becomes tamper proof. As such the present invention is directed to a real world function.

Thus, the subject matter as recited in the claims are directed to permissible statutory subject matter as per 35 U.S.C § 101. Therefore, reconsideration and withdrawal of the 35 U.S.C. § 101 rejection of claims 1, 2 and 6 is respectfully requested.

In view of the foregoing amendments and remarks, applicants submit that claims 1, 2 and 4-6 are in condition for allowance. Accordingly, early allowance of claims 1, 2 and 4-6 is respectfully requested.

In view of the foregoing amendments and remarks, Applicants submit that all pending claims in this application are in condition for allowance. Accordingly, an early indication of such allowance is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.42884X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120